Remarks

Consideration of the amended claims is respectfully requested. Claims 1-15 are pending, stand rejected, and have been amended in response to the current rejections. New claim 16 has been added for clarification, and is presented for review, as no new matter has been added. Support for the amended language as well as that of Claim 16 may be found on page 3 and page page 10 of the application as filed, as well as other areas of the application as filed and the relevant drawings.

Claims 1-2 and 7-15 stand rejected under 35 USC 102 (e) as being anticipated by Thorsen, U.S. Patent number 6,052, 688. Applicant generally traverses this rejection, but has amended the claims to clarify the claimed invention. Generally, Thorsen discloses a system and method for accessing a database by initiating and maintaining data access nodes and variable access structure. The disclosure in Thorsen is limited to direct access of the database as well as maintaining access structures within the database. Thorsen further teaches methods of securely accessing a database directly to retrieve data.

Claim 1 has been amended to include "an application server configured to control access to data stored in the database and to set up and send a document file having a representation of an object and associated documents that are stored in the database." Emphasis added. According to the invention, direct access to the database by a user is not required. Rather than giving a user limited access to a database, the invention provides a system whereby an application server packages a representation of an object in a document file that contains a version of the object along with representations of any associated documents. These limitations are clarified in Claim 1, that is limited by "access data application code stored in the memory and executable by the application server, the application code being responsive to the access criteria associated with the groups of data contained within a version of an object and to predetermined privileges for allowing controlled access to individual groups of data contained within the version of the object by an individual user that was set up to be sent to a user computer system and that may be viewed by a user according to the user's predetermined privileges on the user computer system." Thorsen does not disclose or suggest the limited access of an object that is outside the database. Thorsen discloses methods of controlled access to data items that reside in the database, not limited access on the user's computer. Accordingly, applicant respectfully requests that the rejection of Claim 1 under 35 USC 102(e) over Thorsen be withdrawn.

7

Claim 2 depends from Claim 1, incorporates the amended limitations of Claim 1, and has been further amended to read as follows: "wherein the access data application code enables [includes] the ability of a user to read the contents of the transferred version of the requested object that was sent by the application server according to access privileges associated with the user." Thus, Claim 2 further clarifies that the version of the object is transferred to a user by the application server for access outside the database. This is not disclosed or suggested in Thorsen. Accordingly, applicant respectfully requests that the rejection of Claim 1 under 35 USC 102(e) over Thorsen be withdrawn.

Claim 7 has been amended to include similar limitations of Claim 1 as follows:

controlling the access to the database using a [central processing unit(CPU)] an application server, that is configured to set up a version of an object according to access criteria established for a user;

storing software code for controlling the operation of the CPU in memory;

transferring a version of an object to a user in the form of a document file having the version of the object and any associated documents requested by a user contained therein; and

allowing controlled access to individual groups of data contained within the transferred version of the object by an individual user according to [the] an individual user's predetermined privileges in response to the access criteria associated with the groups of data contained within [an] the version of the object transferred to the user and to a user's predetermined privileges.

Similar to Claim 1, Claim 7 is limited to versions of an object that are transferred to a user, wherein access to the object is limited to predetermined privileges of a user. Accordingly, applicant respectfully requests that the rejection of Claim 1 under 35 USC 102(e) over Thorsen be withdrawn.

Claim 8 depends from Claim 7, incorporates the amended limitations of Claim 7, and has been further amended to include the limitations as follows:

receiving an object request by a requestor;

verifying the requestor's user privilege access criteria; and

8

transmitting [information] a version of an object configured to reveal information contained with in the version of the object according to the requestor's user privilege access criteria.

Thus, Claim 8 further clarifies that the version of the object is transferred to a user by the application server for access outside the database. This is not disclosed or suggested in Thorsen. Accordingly, applicant respectfully requests that the rejection of Claim 1 under 35 USC 102(e) over Thorsen be withdrawn.

Claim 9 also depends from Claim 7 and further includes further limitations that have been amended to read "wherein establishing [an] a version of an object includes loading information into the version of the object into separate groups having separate access privilege criteria." Accordingly, applicant respectfully requests that the rejection of Claim 1 under 35 USC 102(e) over Thorsen be withdrawn.

Claim 10 depends from Claim 7 and includes the further limitation where a "user may access for use in setting up a version of the object to be sent to the user in response to the user request." Thus, Claim 10 further clarifies that the version of the object is transferred to a user by the application server for access outside the database. This is not disclosed or suggested in Thorsen. Accordingly, applicant respectfully requests that the rejection of Claim 1 under 35 USC 102(e) over Thorsen be withdrawn.

Claim 11 depends from Claim 7 (the examiner is referred to the above comments related to Claim 7), and contains the further limitation "wherein verifying the requestor's user privilege access criteria includes extracting the requestor's user identification from the object request, verifying the requestor's user identification and identifying the groups of data within the version of the object to which the requestor has access." Accordingly, applicant respectfully requests that the rejection of Claim 1 under 35 USC 102(e) over Thorsen be withdrawn.

Claim 12 depends from Claim 7 that includes the further limitation by "further comprising transmitting a redacted version of an object [includes] by sending an electronic object to the requestor that contains the groups of information to which the requestor has access to and that excludes groups of information associated with an object to which the requestor does not have access." Thus, Claim 12 further clarifies that the version of the object is transferred to a user by the application server for access outside the database. This is not disclosed or suggested in Thorsen. Accordingly, applicant respectfully requests that the rejection of Claim 1 under 35

9

USC 102(e) over Thorsen be withdrawn.

Claim 13 has been amended as follows:

13.(Amended) A computer program product for use with a computer system, a central processing unit and means coupled to the central processing unit for storing a database to automatically manage objects for viewing and marking an object having varying formats without the use of any originating application of a file to view the object, comprising:

computer readable code means for establishing an object in a storage location;

computer readable code means for identifying a user to have limited access to information associated with the object;

computer readable code means for establishing privilege access criteria that define the scope of access of a version of the object for the user;

computer readable code means for receiving an object request by a requestor;

computer readable code means for verifying the requestor's user privilege access criteria; and

computer readable code means for transmitting a version of the requested object in the form of a redacted document that masks information according to the requestor's user privilege access criteria.

Similar to Claims 1 and 7, Claim 13 is limited to versions of an object that are transferred to a user, wherein access to the object is limited to predetermined privileges of a user. Accordingly, applicant respectfully requests that the rejection of Claim 1 under 35 USC 102(e) over Thorsen be withdrawn.

Claim 14 has been amended as follows:

14. (Amended)   A computer program device, comprising:

a computer program storage device readable by a digital processing apparatus;

a program stored on the program storage device and including instructions executable by the digital processing apparatus for controlling the apparatus to perform a method of managing documents for viewing and [marking] modifying

10

an object [having varying formats without the use of any originating application of a file] to allow a user to view and modify a version of the object stored in the file, comprising:

   establishing an object in a storage location;

   identifying a user to have access to the object;

   establishing privilege access criteria that define the scope of access of a version of the object for the user;

   receiving a object request by a requestor;

   verifying the requestor's user privilege access criteria; and

   transmitting a redacted version of a requested object in the form of a document file containing the version of the requested object that was filtered according to the requestor's user privilege access criteria.

Similar to Claims 1, 7 and 13, Claim 14 is limited to versions of an object that are transferred to a user, wherein access to the object is limited to predetermined privileges of a user. Accordingly, applicant respectfully requests that the rejection of Claim 1 under 35 USC 102(e) over Thorsen be withdrawn.

   Claim 15 has been amended to include the following limitation of "setting up a version of an object and associated documents according to user access privileges for transmission to the user. Claim 15 has also been amended to include "transmitting a redacted version of the requested object that set up according to the requestor's user privilege access criteria, wherein the access criteria defines the information in which a user has privileges of access to the version of the requested object." Similar to the above claims, Claim 15 is limited to versions of an object that are transferred to a user, wherein access to the object is limited to predetermined privileges of a user. Accordingly, applicant respectfully requests that the rejection of Claim 1 under 35 USC 102(e) over Thorsen be withdrawn.

   Claims 3-6 stand rejected under 35 USC 103(a) as being unpatentable over Thorsen. Generally, Applicant traverses this rejection, but has amended Claims 3-6 to clarify the claimed invention. Support for the new language is found on page 3 and page 10 of the application as filed.

   Specifically, Claim 3 depends from Claim 2, which depends from Claim 1, and has been amended as follows: "wherein the access data application code includes the ability to modify the

11

contents of the <u>version of the</u> requested object." Thus the ability to modify is limited to the version of the object sent to a user, and does not include the ability to modify an object I the database as disclosed in Thorsen. The examiner is referred to the amendments to Claim 1 discussed above. Applicant submits that these amendments further distinguish the claimed invention from Thorsen for purposes of the rejections of the 103 rejection as well. Accordingly, applicant respectfully requests that the rejection of Claim 1 under 35 USC 103(a) over Thorsen be withdrawn.

Claim 4 depends from Claim 3, and has been amended as follows: "A system ... wherein the ability to modify includes the ability to delete information contained in the <u>version of the</u> requested object." Thus the ability to modify is limited to the version of the object sent to a user, and does not include the ability to modify an object I the database as disclosed in Thorsen. The examiner is again referred to the amendments to Claim 1 and related discussion. Applicant submits that these amendments further distinguish the claimed invention from Thorsen for purposes of the rejections of the 103 rejection as well. Accordingly, applicant respectfully requests that the rejection of Claim 1 under 35 USC 103(a) over Thorsen be withdrawn.

Claim 5 also depends from Claim 3 and has been similarly amended and the ability to modify has been limited to include "the ability to add data to the <u>version of the</u> requested object." Thus the ability to modify is limited to the version of the object sent to a user, and does not include the ability to modify an object I the database as disclosed in Thorsen. The examiner is again referred to the amendments to Claim 1 discussed above. Applicant submits that these amendments further distinguish the claimed invention from Thorsen for purposes of the rejections of the 103 rejection as well. Accordingly, applicant respectfully requests that the rejection of Claim 1 under 35 USC 103(a) over Thorsen be withdrawn.

Claim 6 depends from Claim 1, and has been amended to include the limitation "wherein the access <u>to the version of the object</u> is determined by a business relationship to produce products and defined by the host according to the need of information in the product <u>chain, and wherein the transferred version of the object is configured to reveal limited information according to a guest user's predetermined access privileges.</u>" Thus, the invention as now claimed is limited to the transferring of a version of an object, where the object is configured to only reveal limited information that is prescribed according to the user's access privileges. Thorsen does not disclose or suggest this limitation. The examiner is referred to the

12

amendments to Claim 1 discussed above. Applicant submits that these amendments further distinguish the claimed invention from Thorsen for purposes of the rejections of the 103 rejection as well. Accordingly, applicant respectfully requests that the rejection of Claim 1 under 35 USC 103(a) over Thorsen be withdrawn.

Accordingly, Applicant respectfully requests that the rejection of Claims 1,2 and 7-15 under 35 USC 102(e) be withdrawn, that the rejection of Claims 3-6 under 35 USC 103(a) be withdrawn, and that Claims 1-16 be allowed.

Applicant further requests and extension of time of two months, at a charge of $400.00, which may be charged to Deposit Account No. 50-1610.

The Commissioner is hereby authorized to charge any additional fees due or credit any overpayment to Deposit Account No. 50-1610.

If there are any questions regarding this correspondence, please contact the undersigned at (408) 288-7588.

Dated June 3, 2002

David R. Stevens
Reg. No. 38,626

Stevens & Westberg, LLP
99 North First Street, Suite 201
San Jose, CA 95113
(408)288-7588
Fax (408)288-7542

13

Clean Version of Claims:

1   1. (Amended) A system for providing the transfer of and the controlled access to a version of an

2   object and other associated information a file by a plurality of users comprising:

3   a database for storing an object and associated information, the object comprising

4   distinguishable groups of data, each group of data having associated access criteria for access to

5   the groups of data;

6   an application server configured to control access to data stored in the database and to set

7   up and send a document file having a representation of an object and associated documents that

8   are stored in the database ;

9   a memory for storing software code for controlling the operation of the application

10   server;

11   access data application code stored in the memory and executable by the application

12   server, the application code being responsive to the access criteria associated with the groups of

13   data contained within a version of an object and to predetermined privileges for allowing

14   controlled access to individual groups of data contained within the version of the object by an

15   individual user that was set up to be sent to a user computer system and that may be viewed by a

16   user according to the user's predetermined privileges on the user computer system.

1   2. (Amended) A system according to Claim 1, wherein the access data application code

2   enables the ability of a user to read the contents of the transferred version of the requested object

3   that was sent by the application server according to access privileges associated with the user.

1   3. (Amended) A system according to Claim 2, wherein the access data application code

2   includes the ability to modify the contents of the version of the requested object.

1   4. (Amended) A system according to Claim 3, wherein the ability to modify includes the

2   ability to delete information contained in the version of the requested object.

1   5. (Amended) A system according to Claim 3, wherein the ability to modify includes the

2   ability to add data to the version of the requested object.

14

1   6. (Amended) A system according to Claim 1 wherein the access to the version of the

2   object is determined by a business relationship to produce products and defined by the host

3   according to the need of information in the product chain, and wherein the transferred version of

4   the object is configured to reveal limited information according to a guest user's predetermined

5   access privileges.

1   7. (Amended) A method of controlling access to objects stored in electronic form,

2   comprising:

3   storing an object, the object comprising distinguishable groups of data, each group of

4   data having associated access criteria for access to the groups of data;

5   controlling the access to the database using an application server, that is configured to set

6   up a version of an object according to access criteria established for a user;

7   storing software code for controlling the operation of the CPU in memory;

8   transferring a version of an object to a user in the form of a document file having the

9   version of the object and any associated documents requested by a user contained therein; and

10   allowing controlled access to individual groups of data contained within the transferred

11   version of the object by an individual user according to an individual user's predetermined

12   privileges in response to the access criteria associated with the groups of data contained within

13   the version of the object transferred to the user and to a user's predetermined privileges.

1   8. (Amended) A method according to Claim 7 further comprising:

2   receiving an object request by a requestor;

3   verifying the requestor's user privilege access criteria; and

4   transmitting a version of an object configured to reveal information contained with in the

5   version of the object according to the requestor's user privilege access criteria.

1   9. (Amended) A method according to Claim 7, wherein establishing a version of an

2   object includes loading information into the version of the object into separate groups having

3   separate access privilege criteria.

1   10. (Amended) A method according to Claim 7, wherein establishing privilege

2 access criteria includes identifying the separate groups of information to which the user may

3 access for use in setting up a version of the object to be sent to the user in response to the user

4 request .

1   11. (Amended) A method according to Claim 7, wherein verifying the requestor's

2 user privilege access criteria includes extracting the requestor's user identification from the

3 object request, verifying the requestor's user identification and identifying the groups of data

4 within the version of the object to which the requestor has access.

1   12. (Amended) A method according to Claim 7, further comprising transmitting a

2 redacted version of an object by sending an electronic object to the requestor that contains the

3 groups of information to which the requestor has access to and that excludes groups of

4 information associated with an object to which the requestor does not have access.

1   13.(Amended) A computer program product for use with a computer system, a central

2 processing unit and means coupled to the central processing unit for storing a database to

3 automatically manage objects for viewing and marking an object having varying formats without

4 the use of any originating application of a file to view the object, comprising:

5   computer readable code means for establishing an object in a storage location;

6   computer readable code means for identifying a user to have limited access to

7 information associated with the object;

8   computer readable code means for establishing privilege access criteria that define the

9 scope of access of a version of the object for the user;

10   computer readable code means for receiving an object request by a requestor;

11   computer readable code means for verifying the requestor's user privilege access criteria;

12 and

13   computer readable code means for transmitting a version of the requested object in the

14 form of a redacted document that masks information according to the requestor's user privilege

15 access criteria.

16

1   14. (Amended) A computer program device, comprising:

2   a computer program storage device readable by a digital processing apparatus;

3   a program stored on the program storage device and including instructions executable by

4 the digital processing apparatus for controlling the apparatus to perform a method of managing

5 documents for viewing and modifying an object to allow a user to view and modify a version of

6 the object stored in the file, comprising:

7   establishing an object in a storage location;

8   identifying a user to have access to the object;

9   establishing privilege access criteria that define the scope of access of a version of the

10 object for the user;

11   receiving a object request by a requestor;

12   verifying the requestor's user privilege access criteria; and

13   transmitting a redacted version of a requested object in the form of a document file

14 containing the version of the requested object that was filtered according to the requestor's user

15 privilege access criteria.

1   15. (Amended) In a computer server having a data base for storing data pertaining

2 to product information, a method of securely transferring data between a source and an access

3 destination comprising:

4   establishing an object in a storage location;

5   identifying a user to have limited access to the object;

6   establishing privilege access criteria that define the scope of access of a version of the

7 object for the user;

8   receiving a object request by a requestor;

9   verifying the requestor's user privilege access criteria;

10   setting up a version of an object and associated documents according to user access

11 privileges for transmission to the user; and

12   transmitting a redacted version of the requested object that set up according to the

13 requestor's user privilege access criteria, wherein the access criteria defines the information in

14 which a user has privileges of access to the version of the requested object.

17

1   16. (New Claim)   In an application server having access to a data base for storing objects

2   and associated documents, a method of securely transferring a version of an object and

3   associated documents from the application server to a user system via a network comprising:

4   establishing privilege access criteria that define the scope of access permitted to a user of

5   a version of an object that may be set up and sent to the privileged user;

6   receiving a object request by a user via a network for access to a version of an object to

7   which the user has access privileges;

8   verifying the requestor's user privilege access criteria;

9   setting up a version of an object and associated documents according to user access

10   privileges for transmission to the user; and

11   transmitting a version of the requested object that was set up according to the requestor's

12   user privilege access criteria in the form of a document file that includes a version of the

13   requested object and a version of associated documents via the network.

18